ПРОБЛЕМИ БОРОТЬБИ З КОМП'ЮТЕРНИМИ ВІРУСАМИ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Ткачова О. К., *канд. наук держ. упр.,* ***Лосєв В. Д.,*** *студент, Університет митної справи та фінансів*

Віруси були і залишаються серйозною проблемою, а особливо в умовах діджиталізації. І для суб'єктів господарювання актуальним є питання захисту та збереження інформації від вірусів та кібератак. Адже, як казав Натан Ротшильд «Хто володіє інформацією, той володіє світом». Інформація в сучасному суспільстві є на даний момент одним з найцінніших продуктів. Тому проблеми збереження і захисту інформації є дуже важливими і хвилюють кожного від школяра до президента країни [3].

Чому виникають комп'ютерні віруси? Як уберегти свій комп'ютер від них? Чи є антивірусні програми ефективним засобом захисту і, які з них, кращі? Ось такими питаннями можна «окреслити» коло проблем, що виникає перед кожним користувачем комп'ютера. Віруси і шкідливі програми постійно розвиваються і щодня стають більш витонченими і небезпечними, що значно ускладнює захист даних. Якщо комп'ютер немає надійного захисту, користувач ризикуєте стати жертвою атак новітніх комп'ютерних вірусів і шкідливих програм.

Кіберзлочинці невблаганні і постійно намагаються зламати комп'ютери і телефони з метою крадіжки цінних даних – банківських реквізитів, особистих фотографій і важливих документів. Тому необхідно мати працюючий антивірус на комп'ютері, пристрої Mac, Android або IPhone.

Розглянемо від яких найнебезпечніших комп'ютерних вірусів і нових шкідливих програм слід захищатися в 2020 році [1].

1. Програма-вимагач Clop.

Clop – це шкідлива програма, яка шифрує файли і вимагає заплатити викуп хакерам за розблокування. «Clop» є однією з новітніх шкідливих програм. Вона є різновидом добре відомої програми-здирника CryptoMix, яка часто робить атаки на користувачів Windows. Програма-вимагач Clop розвивається з моменту своєї появи і вже здатна атакувати цілі мережі замість окремих пристроїв. Жертвою програми-Clop став навіть Маастрихтський університет в Нідерландах – практично всі пристрої мережі з операційною системою Windows виявилися заблокованими з метою отримання викупу.

2. Підставні поновлення Windows (приховані програми-вимагачі). Останнім часом хакери все частіше відправляють електронні листи з проханням встановити термінове оновлення ОС Windows. Листи обманом змушують користувачів встановити «останні» оновлення Windows, які насправді є замаскованими програмами-вимагачами в форматі '.exe'. Така відома програма-вимагач Кіборг (Cyborg) шифрує всі файли і програми і вимагає викуп за розблокування файлів. На жаль, багато постачальників служб електронної пошти і базові антивіруси не здатні виявити і заблокувати подібні електронні листи.

3. Zeus Gameover.

Zeus Gameover є однією з різновидів вірусів і шкідливих програм сімейства «Zeus», що маскується під звичайну програму і отримує доступ до банківських даних і краде кошти. Найгірше, що для даного різновиду шкідливих програм для здійснення транзакцій не потрібен доступ до централізованого сервера. Це є слабким місцем багатьох кібератак, що відслідковуються державними органами. Замість цього, Zeus Gameover обходить центральні сервери і створює незалежні сервери для відправки конфіденційної інформації.

4. Атаки новинних шкідливих програм.

Атаки новинних шкідливих програм проходять через актуальні новини та світові події для зараження комп'ютерів шкідливими програмами. Одним із прикладів є атаки хакерів на звичайних користувачів за допомогою шкідливих програм під прикриттям інформації про спалах COVID-19 (коронавірус). Хакери відправляють електронні листи, замасковані під офіційну інформацію про епідемію. Читачів просять перейти по посиланню для отримання докладної інформації, однак посилання містить шкідливу програму, яка копіює файли на пристрій і краде персональні дані. В даний час дослідження націлені на вивчення поширення цієї шкідливої програми в Японії. При цьому, під час будь-яких подій, що залучають багато уваги, подібні програми можуть стати світовою проблемою.

5. Fleeceware.

Це шкідливі програми, які знімають з рахунків користувачів додатків великі суми навіть після видалення даних додатків. Недавні дослідження показали, що за останні роки понад 600 мільйонів користувачів Android завантажили Fleeceware на свої пристрої. Незважаючи на те, що Fleeceware не представляє смертельної загрози безпеки пристроїв і даних користувача, вони дуже поширені і є прикладом недобросовісної практики розробників додатків зібрати гроші з користувачів, які нічого не підозрюють.

6. Атаки з використанням штучного інтелекту (AI).

Сьогодні з'являється все більше інструментів для написання AI скриптів і програм, що дає хакерам можливість використовувати дану технологію для проведення потужних атак. Дані технології також можуть бути використані для злому пристроїв і мереж у величезних масштабах.

Особливого захисту в умовах постійних кібератак потребують цінні конфіденційні дані користувача, банківські реквізити, особисті фото і повідомлення.

Більшість користувачів застосовують лише базові антивіруси і окремі інструменти забезпечення кібербезпеки. Однак правда в тому, що більшість антивірусних програм не забезпечує 100% захист від нових шкідливих програм – швидше за все, користувачі ще уразливі для новітніх вірусних загроз.

Для забезпечення безпеки пристрою і даних необхідно використовувати кращі антивіруси для комп'ютера, Mac, Android, і iOS пристрої.

Під деякими антивірусами ховаються шкідливі програми, які створені з метою крадіжки персональних даних. Це особливо актуально для Windows, оскільки через величезної кількості користувачів по всьому світу, Windows є

найпопулярнішою мішенню для вірусів і інших шкідливих програм. Тому особливо важливо не стати жертвою однієї з таких шахрайських програм і завантажувати тільки справжні програми з великою історією добросовісної роботи на ринку.

Однак, з огляду на зростання кіберзлочинів, в даний час є лише кілька безкоштовних антивірусів для Windows, що пропонують гідний захист ПК.

Оскільки немає такого поняття, як «безкоштовний антивірус» без обмежень, п’ять світових компаній пропонують безкоштовний тариф. Хоча найчастіше вони мають лише базові функції, більшість з них варто спробувати, при тому, що деякі з них набагато краще, ніж Захисник Windows – стандартна програма забезпечення захисту Windows.

Список кращих безкоштовних антивірусів для Windows в 2020 р. [2]:

1) Panda: 1 місце в списку кращих безкоштовних антивірусів для Windows для більшості користувачів в 2020 році;

2) Avira: відмінна технологія, що забезпечує надійний захист від вірусів і шкідливих програм;

3) Sophos: кращий безкоштовний сімейний тариф. Відмінний інтерфейс з батьківським контролем (до 3 пристроїв);

4) Kaspersky: корисні додаткові функції, такі як VPN, моніторинг даркнета і менеджер паролів;

5) Bitdefender: найпростіший безкоштовний антивірус з низьким навантаженням на процесор [2].

Насправді, багато компаній забезпечують найвищий рівень захисту тільки користувачам платних версій – такими компаніями, в тому числі, є Malwarebytes і TotalAV.

Існують ще антишкідливі програми, які схожі на антивіруси, але не ідентичні їм. Антишкідливі програми борються як з традиційними вірусами, так і з усіма численними інтернет-атаками сучасних кіберзлочинців. Тим не меньше, більшість компаній, що займаються кібербезпекою, взаємозаміняють терміни «антивірус» і «антишкідлива програма». Останнє рекламується як «антивірус», але насправді є антишкідливим програмним забезпеченням.

Антивіруси і антишкідливі програми (antimalware) були створені для виявлення і захисту від шкідливих програм. Хоча термін «антивірус» означає, що він захищає тільки від комп'ютерних вірусів, його функції часто дозволяють захищати від багатьох інших форм шкідливих програм, поширених в наші дні. Захист від шкідливих програм йде ще далі і фокусується на більш широких, більш складних загрозах. Для розуміння ситуації, це як антивірус, але тільки додатково оновлений і посилений для виявлення нових шкідливих програм і ефективного захисту від них [4].

Захист від шкідливих програм і антивірус – це не одне і те ж. Вони доповнюють один одного, щоб забезпечувати найвищий рівень захисту від шкідливих програм, поряд з правильними звичками і поведінкою в Інтернеті самого користувача. Антишкідлива програма виявляє більш просунуті форми шкідливих програм, такі як невідомі атаки «нульового дня», в той час як антивірусне програмне забезпечення захищає від традиційних, відомих загроз.

Далеко не всі антивірусні продукти, які можна виявити на полицях магазинів або в мережі, дають захист, близьку до 100%. Більшість продуктів не гарантує навіть 90% -вий рівень захисту. В цьому і полягає основна проблема антивірусних компаній на сьогоднішній день.

При тому, що в середньому в місяць з'являється близько 300 нових різновидів вірусів. В результаті багато антивірусних компаній просто не в змозі встигнути за цим потоком, вони програють у вірусній «гонці озброєнь», а користувачі цих програм виявляються захищені далеко не від усіх сучасних комп'ютерних загроз.

Видалення виявленого шкідливого коду із зараженої системи дуже важко. Часто віруси і троянські програми роблять спеціальні дії, щоб приховати факт своєї присутності в системі, і / або вбудовуються в неї так глибоко, що завдання «виколупуванням кліща» стає досить нетривіальною.

Для того щоб перевіряти файли «на льоту» і постійно захищати підопічний комп'ютер, антивірусним програмам доводиться досить глибоко проникати в ядро системи, причому проникати доводиться в одні і ті ж зони. Говорячи технічною мовою, антивіруси повинні встановлювати перехоплювачі системних подій глибоко всередині захищати системи і передавати результати своєї роботи антивірусного «движку» для перевірки перехоплених файлів, мережевих пакетів та інших потенційно небезпечних об'єктів [5].

Часто вибір антивірусного рішення ґрунтується не на його дизайні, ціні або вдалій рекламі, а на технічних характеристиках, які сильно відрізняються в різних антивірусних продуктах. Основне питання – від яких саме комп'ютерних загроз захищає дане рішення і наскільки якісна надаваний захист.

Список використаних джерел:

1. Андерсон С. 10 новейших вирусов и вредоносных программ в 2020 году. URL: https://ru.safetydetectives.com/blog/novye-virusy-i-vredonosnye-programmy.

2. Джексон С. 5 лучших антивирусов для Windows в 2020 году. URL: https://ru.safetydetectives.com/blog/ .

3. Деркач Я. Компьютерные вирусы и защита от них. URL: https://nsportal.ru/ap/library/nauchno-tekhnicheskoe-tvorchestvo/2014/09/06/referat-kompyuternye-virusy-i-zashchita-ot.

4. Kaspersky: Веб-угрозы. URL: https://www.kaspersky.ru/blog/category/threats/.

5. Касперский Е. Современная антивирусная индустрия и её проблемы. URL: https://securelist.ru/sovremennaya-antivirusnaya-industriya/711/.